MANAV RACHNA INTERNATIONAL UNIVERSITY

TITLE: Study and Analysis of Techniques for Development of Quality of Service in Networks

Synopsis

For

Ph. D. Programme 2011-12

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

FACULTY OF ENGINEERING & TECHNOLOGY

Submitted by:
Name: MEENAKSHI KHASHU
Registration No: 11/Ph.D/0011

Supervisor:
Name: Dr. SURESH KUMAR
Designation: Professor, CSE, MRIU, Faridabad

Abstract

A collection of autonomous computers interconnected for the purpose of communication and resource sharing comprises a Computer Network. The demands of users of computer networks are changing very fast. They want information anytime, anywhere. A lot of applications like audio, video conversation, video streaming, etc. are using the networks for transferring data. These types of applications have special requirements in the terms of reliability, bandwidth, jitter, delay, etc. The network should possess these qualities for satisfying the demands of the users. These qualities in the right proportion comprise Quality of Service (QOS). The Network applications are dependent on reliability of networks i.e Quality of Service (QOS) ensured by the network. As the number of audio and video being sent over networks has increased, the QOS is more important in today's network than it ever was. This results in technique finding to provide reliable network performance and at the same time utilization of network resources efficiently.

Open shortest Path First (OSPF) is one such technique. It is responsible for creating a topological map of the network . Due to its improved efficiency and effectiveness of routing, it is used to give a good network performance. The issues in OSPF are removed in Multiple Routing Configuration (MRC) scheme. It gives assurance for a very swift recovery from node as well as link failure. MRC is based on additional information pertaining to routing in the routers . Once the failure is detected, in MRC, packets are forwarded immediately over already configured next hops. A full guarantee of recovery from any node or link failure is obtained in this scheme. A set of backup configurations is created, by making use of the network graph and related link weights in the MRC. The issues in MRC can be removed by optimization of the route which can lead to reduced operational problems of the network. Genetic Algorithm will be used to solve the problems encountered during optimization.

Keywords: Quality of service (Q.O.S.), Utilization, Measurement, International standard organization (ISO), Open system interconnection (OSI), Acknowledgement (ACK), Open shortest path first (OSPF), Multipath routing configuration (MRC), Transmission Control Protocol (TCP), Genetic Algorithm (GA).

CONTENTS

S.No.	Description	Page No
1	Introduction	1-4
2	Literature Review	4-7
3	Description Broad area	8-15
4	Motivation	15
5	Challenges	16
6	Problem Statement	16
7	Objectives of the Study	16
8	Methodology	16-17
9	Expected Outcome of research	17
10	Proposed time frame (Research Plan)	17
11	References	18-19

Introduction

Computer Network is a collection of autonomous computers interconnected for the purpose of communication and resource sharing (Kini et al. 2009). The interconnection can be done using the public telephone network, dedicated leased lines or any other medium. The transmission media used for interconnection may be wired or wireless. The Communication means the transmission, reception and processing of the data. In today's era, computer networks form the core of modern communication systems. The scope of communication has increased significantly in the past decade and this boom in communication would not be possible without the progressively advancing computer networks.

The demands of users of computer networks are changing very fast. They want information anytime, anywhere. The networks are not only used for merely transferring data, but also for applications having special requirements in the terms of reliability, bandwidth, jitter, delay, etc. The network should possess these qualities for satisfying the demands of the users. These qualities in the right proportion comprise Quality of Service (QOS). Data travelling in a network is said to comprise a flow. A flow seeks to attain QOS in a network (Doi, 2014). The characteristics attributed to a flow are:

1. Reliability- The ability of a network to perform consistently as per specifications defines reliability. Network reliability means accessibility, for customers to carry out end to end functionality and experiencing failure without having an effect on operations. Email, File transfer and Internet Access are sensitive to reliability, whereas Audio/Video conferencing is not.
2. Delay- The time it takes for a data bit to travel across the network, from one node or endpoint to another defines delay. Audio/Video conferencing and remote login need minimum delay.
3. Jitter- When packets of the same flow have different values of delay it is called Jitter. Audio/Video conferencing and remote login are sensitive to delay.
4. Bandwidth- It is the capacity of a network connection for supporting data transfers. Bandwidth is application specific. Video conferencing sends millions of bits per second to refresh a color screen whileas number of bits per second in an email may not be one tenth of a million.

Newer applications are coming up every day and therefore new standards of quality of service are being formed. Even though lots of work on improving the quality of service has been done, but still a scope for improvement is seen.

Customer satisfaction is the main goal of providing a good quality of service. This is achieved by creating a balance between application demand and network performance. If application demand is high and network performance is low, no quality of service is obtained and if application demand is low and network performance is high, it results in wastage of resources. When the application demand is equal to network performance, this results in high quality of service and it is the goal of a network design. As the number of users has increased, the size of internet has also increased and therefore care needs to be taken so that there is no degradation in performance of the network.

Communication scenario is overshadowed by the Internet. Currently the internet is dominated by Transmission Control protocol (TCP) based traffic such as remote terminal, File Transfer Protocol (FTP), Web traffic and Electronic mail. When QOS deteriorates, because of large amounts of data in the network, congestion occurs. Congestion remains a major problem that leads to poor performance.

Networks that are used in our daily lives range from small networks to large internetworks. In other words, it means local to global networks. When at home one can have a couple of computers and a router but an office can comprise of multiple routers and switches which look after communication needs of several hundreds of PCs. Packets of data are forwarded by the routers by making use of information in the routing table. Determination of internet capability is done by the routing protocol. The protocol deals with the following issues:

1. Scalability of internet
2. Swiftness of routing around failures
3. Network resource consumption

The routing protocols can be classified on the basis of:

- Purpose—Interior Gateway and Exterior Gateway Protocol (RIP, BGP).
- Operation—Distance Vector, Link state and Path Vector Protocol (RIP, OSPF, BGP).
- Behaviour--Classful and Classless (RIPV1, OSPF).

Routing Information Protocol (RIP) is the most prevalent IP routing protocol used. Routing loops and slow convergence are the two basic limitations of RIP (Vetriselvan et al. 2014). Furthur RIP cannot be used in large networks. These limitations are responsible for the development of Open Shortest Path First (OSPF). OSPF gives considerable improvements over RIP in the following manner:

- Building a topological map: OSPF is responsible for creating a topological map of the network topology. This means that every router is capable of determining the shortest path to every network by using a shortest path first tree.
- Support for large network diameters: Using hierarchical network design which is based on areas, the network diameter in OSPF is limitless.
- High reliability, routing updates: The updates in OSPF have a high degree of reliability and the reason for that is acknowledgement. In case of the route or link failure, only partial routing updates are sent.
- Equal-cost load balancing**:** OSPF load-shares across equal-cost paths, optimizing bandwidth and multiple paths.

The Routing protocols have a slow convergence rate. This is a serious problem when there is a failure in the network. The technique to address this problem is Multiple Routing Configuration (MRC). Recovering fast from node as well as link failures is the main contribution of MRC and when a node or link fails , packet forwarding continues on an optional link and routers are always equipped with additional information. This method guarantees recovery for all single failure scenarios (Lee et al. 2015).

To plan and manage networks, the most vital task is to optimize the routing strategy. IP networks, which carry mostly real time decisive traffic, always require routes be optimized. This is done to improve quality of service without additional infrastructure cost. Extra care needs to be taken, when local congestion on the link takes place because of an increase or change in load. Optimizing the route can lead to resolving or at least reducing operational problems of the network. Genetic algorithm will be used to solve the problems encountered during optimization. The basic plan is, the adjustment of paths in IP networks with the current load to travel through and therefore improved utilization

of network resources. A genetic algorithm (GA) is a problem-solving strategy that imitates biological evolution (Kumar et al. 2010). When a problem needs to be solved, all the possible solutions to the problem are taken as input to GA. Encoding of these inputs is done and for quantitative evaluation, a fitness function metric is chosen. Evaluation of each of these inputs is done using the fitness function. So some solutions, from the set of random solutions / candidates chosen, may not work at all and therefore need to be deleted. Others are kept for further processing and allowed to regenerate. This regeneration results in certain random changes and therefore some imperfections are gained in the process. This process produces offsprings which are said to be digital in nature. Now the digital offsprings, move to the subsequent generation and form a new set of solutions. These solutions are evaluated using the fitness function. On a random basis some individuals would have improved whereas others need to be removed. The improved candidates are better solutions to the problem being discussed. They are again chosen and after making certain changes randomly, copying over to the next generation takes place. It is believed that there will be an increase in the fitness of the population for every round and hence by repetition of this process thousands of times, a very good solution for the problem will be generated.

Literature Review

Rick et al. (2008) talk about the basic concepts of routing protocols. They mention that routing protocol is used to find all networks in the internetwork in a dynamic fashion and to make sure that all routers share the same routing table. In order to send packets from source to destination, a router should posses destination address, routes to all remote networks and also the best route to all remote networks.

This paper looks at the case of dynamic routing, where the details are exchanged between nodes depending on the routing protocol configured on the node. In order to rate the allegiance/fidelity of the routing information, Administrative distance (AD) is used. It is a value which ranges from 0 to 255 where 0 means most trusted and 255 means that it does not allow any traffic to pass through it. If a particular router receives more than a single update from the same network, then the AD value is checked. The router accepts information from the place where AD value is lower. OSPF has an AD

value of 100 whilst RIP has an AD value of 120. The routing metrics namely hop count, cost, bandwidth, delay, load and reliability form the basis of comparison between protocols.

Zhao et al. (2013) analyzed OSPF convergence due to multiple failure. It is seen that delay in convergence takes place because of protocol timers. Therefore the network operator has to carry out proper configuration of OSPF protocol, keeping two things in mind, network failure scenario and dependency. In other words, a balance is to be maintained between faster convergence and good level of processing overhead.

Zhao looks at Internet infrastructure, making use of OSPF as a routing protocol. Reconvergence in OSPF is divided into four steps, namely failure detection, flooding of LSA, calculation of routes, and routing information base / forwarding information base (RIB/FIB) update. Here if the routing calculation is done immediately, after a router receives Link State Advertisement (LSA), the router can end up doing routing table updates many times because more LSA's are going to be reaching the router. Therefore OSPF uses a timer called Shortest path first delay (SPF Delay) to cause a delay in first routing calculation after receiving new LSA's by the router. When more LSA's are received right after first routing calculation, the upcoming calculations are delayed by a timer called SPF Hold. This SPF throttling scheme is used to delay SPF calculation during network instability. Reducing the value of these timers can give fast convergence in case of a single failure, but can cause large amount of routing calculations with large delays in case of multiple failures.

Vetriselvan et al. (2014) have performed a simulation study of OSPF, EIGRP, IGRP and RIP. It is clear that considering router overheads, IGRP have the maximum overhead followed by EIGRP, OSPF and RIP. The OSPF has the highest throughput, followed by EIGRP, IGRP and RIP. The EIGRP has the least delay followed by OSPF, RIP and IGRP and in the case of link utilization, EIGRP has the maximum link utilization and on its heels are OSPF, IGRP and RIP.

An extensive survey on RIP, OSPF and EIGRP routing protocols is carried out in this paper. It is seen that OSPF and EIGRP carry out a distribution of routing information

between routers in a same autonomous system. It looks at an approach to tune dynamic routing system by making use of link metrics. This paper presents the decision taken when a choice is to be made for using distance vector or link state protocol. Here the convergence delay caused due to failure of link for OSPF and EIGRP is compared.

Kvalbein et al. (2006) have discussed a method called Multiple Routing Configuration to take care of the slow convergence rates of routing protocols in case of link/node failure, in a network. The Multiple Routing Configuration (MRC) is a technique which helps IP networks to recover fast from link and node failures. In MRC, packet forwarding persists on an optional link as soon as a failure is detected and additional information is always contained in the routers. The MRC ensures recovery from all single failures and a single mechanism is used for both node and link failure. The MRC uses destination based hop-by-hop forwarding.

Kumar et al. (2011) have discussed an enhanced MRC (EMRC) scheme which supports multiple node or multiple link failure. It takes care of data transmission in IP networks without wasting time in global reconvergence. This technique provides support for multiple failures by utilizing time slot mechanism. Initially OSPF is used for routing. Whenever node or link fails the complete transmission collapse can occur. EMRC uses time slot which means that some time is given for the route to recover before changing the route. If failure recovers within time slot, the data is transmitted in the original route, but if not, then the backup route is chosen and probing is sent to failure recovery. When failure of node/link is set right, the backup route is stopped and original route is chosen. This improves the fastness of routing as backup route is longer than the original route.

Cicic et al. (2007) state that Multi topology routing is a very important network management concept that takes care of transportation of various types of traffic over every network path which is disjoint. They have discussed Relaxed MRC (RMRC) which is better than the MRC in terms of path length and distribution of load between links. It provides faster rerouting in presence of multiple failures. There is no

requirement of every link being isolated in a backup topology in RMRC. This paper also presents a comparison between MRC and relaxed MRC. Relaxed MRC requires lesser backup topologies, better link and node fault tolerance. This reduces the backup path length in RMRC. As the load distribution is better in RMRC, it has lower link utilization in failure cases.

Gonen et al. (2011) analyzed the routing operation taking place on the internet. When data is sent from source to destination, the complete information is divided into chunks called packets. The header information in the form of an IP address is attached to the packet. The data packets are then made to travel on the links towards the routers. The incoming data is then stored in queue before being processed by a particular router. It is the router which reads the IP address and determines the best way to forward the packet to its destination. They have analyzed the algorithm for a network topology of 20 nodes and 62 links and it finds a shortest path in minimum time.

Obeidat et al. (2014) have discussed a routing algorithm for networks based on a combination of GA and network delay analysis. The reason for going onto GA is that it gives better solutions in spite of changes in network topology, that is the addition or deletion of nodes or link and volume of the network. In his methodology the configuration of the network is chosen, based on Multiparameter encoding scheme. For all the combination of nodes, a routing table is created. The various entries in the routing table correspond to the paths between node pairs.

Fadil (2010) states that evaluation of each path is done on the basis of cost (shortest path) to find the routes in most of routing algorithms. If there is overloading or congestion in the shortest path, optimization based on other parameters needs to be carried out to get better solutions. The technique provides alternative paths instead of overloaded paths, so that there is better utilization of network resources and thereby improved QOS. The chromosomes of varying length and their genes are used for encoding purposes. Crossover and mutation provide a searching facility giving an improvement in solution quality and fast convergence.

Description Broad Area

A routing protocol is defined, by a set of rules, that are followed by routers so that they can determine, the most suitable path for packets of data, to be forwarded to the intended destination. Routing protocols are responsible for facilitating router communication and overall network topology understanding (Graziani et al. 2008). Evolution of routing protocols, has occurred over several years, in order to meet the demands of changing network requirements. Migration to recent protocols like Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), has taken place by most of the organizations, but earlier distance vector protocols, such as Routing Information Protocol (RIP), are still in use today. Certain parameters of interest in these protocols are namely, Scalability of the internet, Resource consumption and Routing around failures. Open Shortest path First (OSPF) is an IP routing protocol. It is also said to be an Interior Gateway Protocol (IGP) and is used for distributing routing information amongst routers. The basis of OSPF is a link-state technology.

The features of OSPF are:

- Improved efficiency and effectiveness of routing. Routing updates are sent when network topology changes.
- Increasing flexibility of addressing and conservation of IP address space.
- Improves network security.
- Hop count is not limited.

OSPF follows a hierarchy in routing. This hierarchical structure gives a reduced size of database that every router maintains. When a network is small, it consists of one single area, but in case of large networks, it may comprise of more than one area. Every area is made up of a large number of networks and each of these areas put together form an autonomous system which is connected to OSPF backbone. An autonomous system (AS) means a group of routers that use the same Interior Gateway protocol(IGP). Exterior Gateway protocols (EGP) route data between AS's. Link-state routing protocols are capable of copying the database which defines the topology. The local routing

topology is collected by every router in the routing domain and the information obtained is sent in terms of link state advertisements (LSAs). The link state database is generated by every router from these LSA's . Exchange of LSA's between routers takes place for building up and maintenance of its topology database. On the basis of the link state database, a routing table is calculated by each router.

LSA contains the information listed below, about links:

1. Link IP address.
2. Link subnet mask.
3. Remote router ID.
4. Type of link being considered.
5. Metric or Cost assignment of the link.

A complete representation of the topology of the AS is given by a Link state database (LSDB). The link state database contains the number of routers present in the network, the number of interfaces at each router, the link cost and so on. The OSPF routers maintain a link state database synchronization for high efficiency. At the time of initial connection, between two neighbors, synchronization of initial database takes place, to get rid of errors in the routing table, which can lead to routing loops and black holes. When neighbors are forming the first time, OSPF makes use of database exchange. OSPF does not send the complete database, but only LSA headers. They are sent in the form of OSPF database description packets (DD). The next DD packet is sent by the router when the previous packet is acknowledged. After the series of DD packets have been received, which LSAs are recent ones and which LSAs have not been received is known to the router. After this, the router sends a link state request (LSR) packet, so as to request for desired LSAs. The neighbor, then sends LSAs in the requested link state update packets. Once all the updates are received, adjacency amongst neighbors is proved (Krishnan et al. 2013).

After adjacencies are established there is need for informing other routers about LSA changes. OSPF router does this by reliable flooding. At the time of receiving link state

update the OSPF router puts new LSA in its link state database. Acknowledgement packet, is sent by the OSPF router, back to the sender. The router rebundles the LSA and sends it across all the interfaces except the interface at which the LSA was initially received. LSA updation is seen by comparison of sequence numbers. The larger the sequence number, the more recent is the LSA. Whenever flooding by OSPF router takes place, incrementation of the sequence number takes place. After this the maximum age timer is reset by the neighbor, which receives the update.

Refreshing of LSAs take place after every 30 minutes. In case no refreshing takes place, 60 minutes is the time for LSAs to remain in the database. The decision as to whether databases need to be synchronized is taken by OSPF and it depends on a network segment. An example to be taken here is that of, point-to-point links. In such cases, synchronization of databases between routers is a must, but in case of Ethernet, synchronization of network databases takes place between certain neighbor pairs. OSPF has two types of routers, the DR and neighbors, to consider on broadcast multi access networks. There is an adjacency between DR and its neighbors. If there is any failure in DR, all its neighbors try to send hello packets to the DR. When a neighbor sends four hello packets and the DR does not respond, the neighbour detects failure of DR. At this juncture, the election of a new DR, that is backup DR becomes DR, takes place.

As the hello packet interval, is ten seconds and four such packets are sent, therefore it takes forty seconds for failure of DR to be detected by neighbors. It takes forty seconds, for rerouting all the paths, by OSPF, once DR has failed. This is the router dead interval time. Reduction of this time can be done by setting the value of hello packet interval to less than ten seconds on an OSPF router. But after doing so, it has been seen that, lesser value of hello packet interval, gives rise to false alarms. This means that because of discarding hello packets, DR failure is mistaken by neighbors. Every router comes to know about existence as well as, failure detection of its neighbour, through hello packet.

Issues in OSPF:

1. Complexity of configuration: Complexity of this protocol is higher as compared to most of the Distance Vector Protocols This is because, when running OSPF, the need arises to take care of the complexity of network attribute and dividing areas. So the network administrators, need to be very well conversant with data communication and computer networks in order to make OSPF working well.

2. OSPF is not capable of supporting unequal load balance: Link metrics in OSPF are created based on the bandwidth of the link by default. OSPF only picks path with the smallest metric towards the same destination. This is not like EIGRP, which supports the unequal path load balance by configuration (Vetriselvan et al. 2014).

3. High memory: OSPF requires lots of CPU time and memory too, because of usage of Shortest Path First (SPF) algorithm and the ability to maintain multiple routing information copies.

A growing problem arises because of routing protocols, converging slowly after a network fails. This is of large importance because of the internet playing a very important role in the developing communication interface. The issues in OSPF are taken care of by a technique called Multiple Routing Configuration (MRC). It gives assurance for a very swift recovery from node as well as link failure. The root cause of failure is not known in the MRC.

Hop by hop forwarding is followed in the MRC and it uses additional information pertaining to routing in the routers. Packet forwarding continues on another optional output link as soon as a failure is detected. In MRC, once the failure is detected, packets are forwarded immediately over already configured next hops. A full guarantee of recovery from any node or link failure is obtained in the MRC. A set of backup configurations is created by making use of the network graph and related link weights in the MRC. Manipulation of link weights is done in such a way that for any node/link failure, safe forwarding of packets to the destination is carried out by the node that

detects the failure. Recovery is in milliseconds in MRC and the reason for that is, it is a local and proactive technique.

The main features of MRC are listed below:

- In the case of a failure, the forwarding of packets is continuous. Local rerouting is started immediately by the router that detects the failure and the failure details are not conveyed to the neighbors.
- Availability of the network is improved, by restraining the reconvergence process and also because network failures are short lived.
- MRC is responsible for always finding a route to destination and also handles both node and link failure using a single mechanism (Kvalbein et al. 2006).
- Root cause of failure is not looked into by MRC which means that whether the failure is caused by node or link there is always a preconfigured next-hop to the destination.
- There are no major modifications required to the existing IGP routing protocols for implementing MRC.

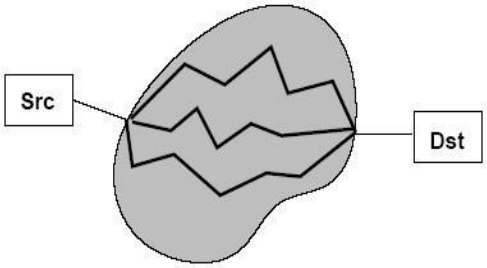

Figure 2: Multiple Routing Configuration

Configuration is a collection of link weights when the original topology is considered. For a particular configuration, which is resistant to a node 'n' failure, assignment of link weights is carried out so that no traffic is routed through the use of 'n'. So when node 'n' fails, it affects only the traffic sent to and sent from 'n'. When a configuration is such that it is resistant to link 'l' failure, no traffic is routed over link 'l' and therefore when link 'l' fails no traffic is lost. Thus, for a configuration node 'n' and link 'l' are isolated in MRC and from this configuration, no traffic is sent through 'n'/ 'l'.

The following are the three main steps involved in an MRC approach:

1. A collection of backup configurations is created and for every configuration, there will be one network component which will not be included for the forwarding of packets.
2. After this OSPF is used for calculation of shortest paths for every configuration and consequently calculation of the router specific forwarding table is carried out. By using a standard protocol for routing, it ensures packet forwarding to go loop free for a particular configuration (Kumar et al. 2011).
3. Next, a forwarding process is designed which gives a fast recovery from network component failure by taking advantage of backup configurations.

The properties of backup configuration are as discussed below:

Firstly the nodes that are not isolated are connected internally by a subgraph which does not include any restricted or isolated link. This subgraph comprises the backbone of the configuration. Secondly, all the links connected to an isolated node will be either isolated or restricted but there will be at least one restricted link connecting the isolated node to the backbone. By making use of the shortest path calculation every router generates a forwarding table which is configuration specific. This means that all the packets are forwarded based on the respective forwarding table calculations which are configuration specific. A router does not immediately inform the rest of the network about its failure to reach a neighbor through one of its interfaces. Instead the packets that were supposed to be sent through the failed interface are identified and specifically marked to belong to a particular backup configuration and another optional route is chosen to send the same towards its destination. This clarifies that all the routers which are down the path are aware of the configuration they have to use. In case of no failure all the packets are forwarded as per the original configuration. So in such circumstances, the failure free original routing, where the normal link weights are used, does not get affected by MRC. In case of a failure, the traffic reaching it, will have to switch configuration (Pham et al. 2003). In order to obtain steady routing, the backup configurations in MRC must stick to the following requirements:

1. In a configuration if a particular node is isolated it cannot carry transit traffic. However, traffic should reach and depart from an isolated node.
2. When a link is isolated in a configuration, it should not carry any traffic.
3. There has got to be a path that connects all node pairs without passing through an isolated node or link, in every configuration.
4. Isolation in at least one backup configuration is a must for every node and every link.

Weights on the restricted links is the first concern. In order that isolated node has no path going through it, it is important that the weight W of restricted link is at least the sum of all link weights in the original configuration:

$$W > \sum w_{ij}$$

This is to guarantee that the shortest path algorithm chosen would allow a path between a node pair which does not pass through the isolated node. As no shorter path exists for packets to be sent to or received from the isolated node, therefore the packets will pass through the restricted link with weight W. The next requisite is that isolated links have an infinite weight so that no traffic is routed through it. After this, an algorithm is used for making all nodes and links isolated in at least one configuration. Network graph G and the number of backup configurations 'n' that are to be created is the input for the algorithm. The algorithm loops all the way through the nodes in the topology and tries to isolate the nodes one at a time. Both the nodes and their attached links are isolated in the same iteration. The algorithm makes sure that all nodes and links in the network are isolated in exactly one configuration. The two invariants are evaluated, whenever a new node and the links are isolated for a particular configuration in the algorithm.

1) For every configuration, a backbone must exist.
2) At least one restricted link, should connect every isolated node, to the backbone.

If these two requirements are not met, then isolation of the node cannot take place in that configuration. The first invariant means that when a new node is isolated, the sub-graph of non-isolated nodes is not divided.

Issues in MRC:

1. Constrained Routing: For generation of back up topology, every link needs to be excluded from routing. These links are said to be isolated in this topology with

weight set to be infinity. Many isolated links are present in a typical backup topology. This constrains the routing of recovered traffic.

2. Load distribution needs to be improved: Link weights can be set independently for multi-topology routing . This tells us that routing of traffic can be done differently, with different sets of link weights for recovery and normal phase. This allows independent traffic engineering for each topology. If link weights are tuned they can be made to improve load distribution. This ability needs to be improved.
3. MRC guarantees recovery in all single failure scenarios, but is not able to handle multiple link and node failures. Multiple failures belong to a shared risk group (SRG) where the common failures include sharing the same conduit, same fiber, network card or router. Natural disasters, terror attacks, power outages or construction workers accidentally breaking a fiber conduct could be the cause of such failure.

Evaluation of each path is done on the basis of cost (shortest path) to find the routes in most of routing algorithms. In case of overloading or congestion taking place in the shortest path, optimization based on other parameters needs to be carried out to get better solutions. Genetic Algorithm (GA) is an optimization algorithm to solve such problems (Obeidat et al. 2012). The basic solution lies in providing alternative paths instead of overloaded paths, so that there is better utilization of network resources and thereby improved QOS.

Motivation

It is a known fact that the world is growing towards a network information revolution. Networks play a very important role in dictating our lifestyle and comforts. In order to maximize user satisfaction, it is essential to give an improved QOS of networks to every user. When the demand of applications equals the network performance, a good quality of service is the result. One of the most important aspect of QOS is a good routing protocol. It plays a very important role in facilitating communication, transfer of data and network topology understanding. There is a lot of work done in this area, but there is scope of more work. This gives us some motivation for further investigation in this area.

Challenges

In order to improve Quality of Service the primary challenge is network congestion. This gives rise to end to end delay because packets start spending more time in the queue at each hop. When a queue is full, incoming packets start to be dropped resulting in increase in packet loss. The result of this is, limited throughput. If two paths have different number of hops and one path is congested than the other, the destination will observe the significant time difference while receiving packets from the same source. This can lead to unacceptable jitter or delay. Routing and security are also issues which can become real challenges, if not dealt with properly. Unequal distribution of resources is another issue which needs to be taken care of.

Problem Statement

To analyze existing congestion control techniques and to develop an efficient technique by integrating the multipath routing configuration and genetic algorithm.

Objectives of the study

The primary objectives of this research are

- To analyze various quality of service improvement techniques for computer networks.
- To analyze various routing and congestion control techniques.
- To identify the research gaps and to address practical issues that act as a bottleneck for quality of service improvements.
- To develop new routing and congestion control techniques for the improvement of quality of service.
- To compare the existing and proposed techniques using a software tool NS2.

Methodology

- Analyzing the performance of Transmission Control Protocol / FTP Traffic and User Datagram Protocol / Constant bit Rate traffic based communication in

wired networks. Network Simulator-2 (NS-2) will be used for simulation. These protocols will be analyzed based on the parameters namely : Throughput, Packet delivery ratio, Packet loss and Delay.

- The performance of different variants of TCP will be analyzed by performing simulations in NS2.
- The literature review will be analyzed to find the contribution of researchers in the area.
- An efficient technique will be proposed and an algorithm will be implemented using simulator.

Expected Outcome of Research

- An efficient congestion control technique providing better QOS will be designed.
- The proposed algorithm will be compared with existing approaches on the parameters like Load balancing, queuing delay, and utilization of the network.

Proposed Time Frame (Research plan)

Research Plan								
	Sem1 (June12)	Sem2 (Dec12)	Sem3 (Dec 13)	Sem4 (June14)	Sem5 (Dec14)	Sem6 (June15)	Sem7 (Dec15)	Sem8 (June16)
Course work								
Literature Review								
Data collection and study								
Interpretation of data								
Attending and presenting papers at conferences								
Thesis submission								

References

Ahmad, S., & Adli, M. 2009 , 'Comparative Study of Congestion Control Techniques in High Speed Networks' , *International Journal of Computer Science and Information Security*, Vol.6, No. 2.

Barzamini, R. & Shafiee, M. 2011, 'LMI Based Switching Congestion Controller for Multiple Bottleneck Packet Switching Networks', *Journal of American science*, pp. 254-261.

Bryant, S., Shand, M. & Previdi, S. 2008, 'IP Fast Reroute Using Not-Via Addresses', *Internet Draft -notvia-addresses-02.txt*.

Cicic, T., Hansen, A. F., Kvalbein, A., Hartman, M., Martin, R.,Menth, M., Gjessing, S. & Lysne O., 2007, 'Relaxed Multiple Routing Configurations: IP Fast Reroute for Single and Correlated Failures', *Department of informatics, Telenor Research and Innovation Centre, IEEE Transactions on 6(1) pp1-14.*

Doi, H. 2014, 'Study on a Fast OSPF Route Reconstruction Method Under Network Failures' *Springer- Verlag Berlin Heidelberg*.

Fadil, Y. 2010 'Routing using Genetic Algorithm for Large Networks', *Diyala Journal of Engineering Sciences*, Vol-03, pp 53-70.

Gonen, B. 2006, 'Genetic Algorithm Finding the Shortest Path in Networks', *International Conference on Genetic and Evolutionary Methods in Department of Computer Science and Engineering, University of Nevada, Reno, Reno, Nevada, U.S.A.*

Graziani, R., & Johnson, A. 2008, 'Routing Protocols and Concepts: CCNA Exploration Companion Guide', *Pearson Education. London*.

Hinds, A., Atojoko, A. & Zhu, S. 2013, 'Evaluation of OSPF and EIGRP Routing Protocols for IPv6', *International Journal of Future Computer and Communication*.

Kini, S., Ramasubramanian, S., Kvalbein, A. & Hansen, A. 2009, 'Fast Recovery from Dual-Link Failures in IP Networks', *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, Rio de Janeiro, Brazil, pp. 1368–1376.

Krishnan, Y. N. & Shobha, G. 2013, 'Performance Analysis of OSPF and EIGRP Routing Protocols for Greener Internetworking', *International Conference on Green High Performance Computing.*

Kumar, T. A. & Prasad, M. K. 2011, 'Enhanced Multiple Routing Configurations For Fast IP Network Recovery From Multiple Failure', *International Journal of Computer Networks (IJCN)*, Vol 3 , Issue 4.

Kumar, R. & Kumar, M. 2010, 'Exploring GA for Shortest Path Optimization in Data Networks',*Global Journal of Computer Science and Technology*, Vol 10, Issue 11, pp.1-8.

Kvalbein, A., Hansen, A. F., Cicic, T., Gjessing, S. & Lysne, O. 2006, 'Fast IP Network Recovery using Multiple Routing Configurations', *Proceedings of twenty fifth IEEE International Conference on Computer Communications (INFOCOM).* pp. 1–11.

Lee, G. & Choi, J. 2015, 'A Survey of Multipath Routing for Traffic Engineering', Conference on Cloud and Web Services.

Obeidat, A .F. & Alshalabi, M. E. ,2012, 'Improving the Performance of the Networks Using Genetic Algorithm'*, Proceedings of the International Conference on Advances in Computer and Information Technology - ACIT* .

Ohara, Y., Imahori, S. & Meter, R. V. 2009, 'MARA:Maximum Alternative Routing Algorithm', *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, Rio de Janeiro, Brazil, pp. 298–306.

Pham, P. P. & Perreau, S. 2003 'Performance Analysis of Reactive Shortest Path and Multipath Routing Mechanism with Load Balance', *IEEE Explore.IEEE.org INFOCOM.*

Soldatos, J., Vayias. & Kormentzas, G. 2005, 'On the Building Blocks of Q.O.S in Networks', *IEEE Communication survey*, vol 7, No.1.pp 700-710

Vetriselvan, V., Patil, P. R. & Mahendran, M. 2014, 'Survey on RIP, OSPF, EIGRP Routing Protocol', *International Journal of Computer Science and Information Technologies (IJCSIT),* Vol. 5 (2) ,pp. 1058-1065.

Wah, B. 2008, 'Transport Layer Issues', *Wiley Encyclopedia of computer science & Engg,*Vol 2. Pp 261-265.

Ye, Z., Krishnamurthy, S. V. & Tripathi, S. K. 2003, 'A Framework for Reliable Routing in Mobile Adhoc Networks', *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)* , pp.270–280.

Zhao, D., Xiaofeng, H. & Chunqing, W .2013, 'A Study on the Impact of Multiple Failures on OSPF Convergence', *International Journal of Hybrid Information Technology* Vol. 6, No. 3.pp 223-229.